

(19) Organisation Mondiale de la Propriété
Intellectuelle
Bureau international



537 306

(43) Date de la publication internationale
17 juin 2004 (17.06.2004)

PCT

(10) Numéro de publication internationale
WO 2004/052005 A1

(51) Classification internationale des brevets⁷ : H04N 7/16,
7/167

(21) Numéro de la demande internationale :
PCT/IB2003/005654

(22) Date de dépôt international :
1 décembre 2003 (01.12.2003)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
2044/02 3 décembre 2002 (03.12.2002) CH

(71) Déposant (pour tous les États désignés sauf US) : NA-
GRACARD SA [CH/CH]; Route de Genève 22, CH-1033
Cheseaux-sur-Lausanne (CH).

(72) Inventeurs; et

(75) Inventeurs/Déposants (pour US seulement) : BRIQUE,

Olivier [CH/CH]; Chemin de la Perrause 39, CH-1052
Le Mont-sur-Lausanne (CH). GOGNIAT, Christophe
[CH/CH]; Avenue de Préfaully 25A, CH-1022 Cha-
vannes-près-Renens (CH).

(74) Mandataire : LEMAN CONSULTING SA; Route de
Clémenty 62, CH-1260 Nyon (CH).

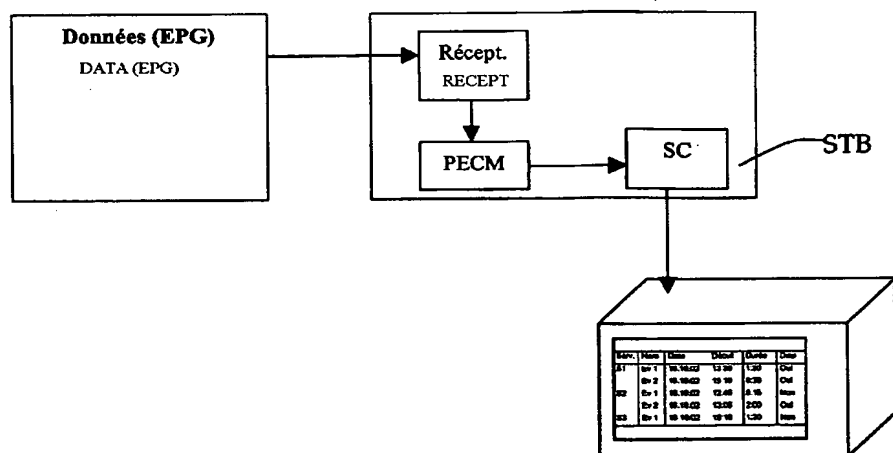
(81) États désignés (national) : AE, AG, AL, AM, AT, AU, AZ,
BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU,
CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE,
GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR,
KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK,
MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT,
RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR,
TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) États désignés (régional) : brevet ARIPO (BW, GH, GM,
KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet
eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet

[Suite sur la page suivante]

(54) Title: METHOD OF MANAGING THE DISPLAY OF EVENT SPECIFICATIONS WITH CONDITIONAL ACCESS

(54) Titre : PROCÉDÉ DE GESTION DE L'AFFICHAGE DE DESCRIPTIFS D'ÉVÈNEMENTS À ACCÈS CONDITIONNEL



(57) Abstract: The invention relates to a method of managing the display of event specifications with conditional access, in order, for example, to display an electronic programme guide for pay television. The inventive method comprises the following steps: (a) data forming an electronic programme guide (EPG) are sent to a decoder (STB), said data containing, for each event, at least one identifier, textual data and a conditional package comprising the conditions required in order to access the aforementioned event; (b) at least one authorisation message (EMM) is sent to a security module (SC) which is associated with the decoder, said message defining the event access rights; (c) the conditional package (PECM) is sent to the security module (SC); (d) the access condition contained in the conditional package (PECM) is processed in the security module; and (e) a message is sent by the security module, which, depending on the access condition for each event and on the access rights contained in the security module, indicates whether or not the right is present for each event in the security module. The method can be used to manage structured language queries as well as enabling the management of complex access conditions.

[Suite sur la page suivante]



européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

Publiée :

— avec rapport de recherche internationale

(57) Abrégé : L'invention a pour objet de gérer l'affichage de descriptifs d'événements à accès conditionnel, notamment pour afficher un guide électronique de programmes pour la télévision à péage. Ce but est atteint par un procédé comportant les étapes suivantes; a) envoi de données formant un guide électronique de programmes (EPG), à un décodeur (STB), ces données comportent, pour chaque événement, au moins un identifiant, des données textuelles et un bloc conditionnel comprenant les conditions requises pour ('accès à cet événement, b) envoi d'au moins un message d'autorisation (EMM) à un module de sécurité (SC) associé au décodeur, ce message définissant des droits d'accès à un événement, c) envoi audit module de sécurité (SC), du bloc conditionnel (PECM), d) traitement, dans le module de sécurité, de la condition d'accès contenue dans ledit bloc conditionnel (PECM), et e) renvoi par le module de sécurité d'un message indiquant, en fonction de la condition d'accès pour chaque événement et des droits d'accès contenus dans le module de sécurité, si le droit est présent ou non pour chaque événement dans le module de sécurité. Ce procédé permet de gérer des requêtes en langage structure et rend possible la gestion de conditions d'accès complexes.

PROCEDE DE GESTION DE L'affichage de DESCRIPTIFS D'evenements A ACCES CONDITIONNEL

La présente invention concerne un procédé de gestion de l'affichage de descriptifs d'événements à accès conditionnel, en particulier pour la
5 télévision à péage.

Dans les systèmes à accès conditionnel, en particulier dans le domaine de la télévision numérique à péage, un flux de données numériques est transmis vers le téléviseur. Ce flux est chiffré afin de pouvoir en contrôler l'utilisation et de définir des conditions pour une telle utilisation. Ce
10 chiffrement est réalisé grâce à des mots de contrôle (Control Words) qui sont changés à intervalle régulier (typiquement entre 5 et 30 secondes) afin de dissuader toute attaque visant à retrouver un tel mot de contrôle.

Pour que le récepteur puisse déchiffrer le flux chiffré par ces mots de contrôle, ces derniers lui sont envoyés indépendamment du flux dans des
15 messages de contrôle (ECM) chiffrés par une clé propre au système de transmission entre un centre de gestion et un module de sécurité de l'unité d'utilisateur. En effet, les opérations de sécurité sont effectuées dans un module de sécurité (SC) qui est généralement réalisé sous la forme d'une carte à puce, réputée inviolable. Ce module peut être soit de type amovible
20 soit directement intégré au récepteur.

Lors du déchiffrement d'un message de contrôle (ECM), il est vérifié, dans le module de sécurité (SC), que le droit pour accéder au flux considéré est présent. Ce droit peut être géré par des messages d'autorisation (EMM) qui chargent un tel droit dans le module de sécurité. D'autres possibilités
25 sont également envisageables telles que l'envoi de clés de déchiffrement.

Pour la suite de l'exposé, on appellera "événement" un contenu vidéo, audio (par exemple MP3) ou données (programme de jeu par exemple) qui est chiffré selon la méthode connue des mots de contrôle, chaque

événement pouvant être chiffré par un ou plusieurs mots de contrôle, chacun ayant une durée de validité déterminée.

La comptabilisation de l'utilisation de tels événements est aujourd'hui basée sur le principe de l'abonnement, de l'achat d'événements ou du paiement par unité de temps.

L'abonnement permet de définir un droit associé à un ou des canaux de diffusion transmettant ces événements et permet à l'utilisateur d'obtenir ces canaux en clair si le droit est présent dans son module de sécurité.

Parallèlement, il est possible de définir des droits propres à un événement, tel qu'un film ou un match de football. L'utilisateur peut acquérir ce droit (achat par exemple) et cet événement sera spécifiquement géré par ce droit. Cette méthode est connue sous l'appellation "pay-per-view" (PPV).

Un message de contrôle (ECM) ne contient pas uniquement le mot de contrôle, mais également les conditions pour que ce mot soit renvoyé au récepteur/décodeur. Lors du déchiffrement des mots de contrôle, il sera vérifié si un droit associé aux conditions d'accès énoncées dans le message est présent dans le module de sécurité.

Le mot de contrôle n'est retourné à l'unité d'utilisateur que lorsque la comparaison est positive. Ce mot de contrôle est contenu dans un message de contrôle ECM qui est chiffré par une clé de transmission.

Pour que le droit soit présent dans le module de sécurité, il est généralement chargé dans ce module par un message d'autorisation (EMM) qui, pour des raisons de sécurité, est généralement chiffré par une clé différente dite clé de droit (RK).

Selon une forme connue de diffusion de télévision à péage, les trois éléments suivants sont nécessaires pour déchiffrer un événement à un moment donné:

- les données relatives à l'événement chiffré par un ou une pluralité de mots de contrôle (CW),

- le ou les messages de contrôle ECM contenant les mots de contrôle (CW) et les conditions d'accès (AC)
- le droit correspondant stocké dans le module de sécurité permettant de vérifier les dites conditions d'accès.

5 Lorsque l'on souhaite rendre visible à un utilisateur, la liste des canaux ou services ou des événements auxquels il a accès, de même que ceux pour lesquels il peut se procurer les droits, les principes décrits ci-dessus sont également utilisés. Pour ceci, on utilise un guide électronique (EPG = Electronic Program Guide) et l'on affiche, par exemple en vert, les
10 événements ou canaux pour lesquels les droits sont déjà acquis et en rouge ceux pour lesquels les droits ne sont pas acquis.

Lorsque la caractérisation des droits est simple, par exemple lorsque l'utilisateur est abonné à certains services prédéfinis pour une durée de validité déterminée, il est aisé de générer un EPG qui tienne compte de ces
15 droits. Par contre, lorsque l'on souhaite gérer des droits plus complexes, réaliser des offres promotionnelles ou utiliser des conditions qui n'ont pas été prévues dans l'abonnement, les systèmes actuels ne permettent pas de gérer facilement ces éléments.

La demande internationale de brevet WO 97/42762 décrit un système
20 d'accès à des informations, qui peut être utilisé notamment dans le domaine de la télévision à péage. Dans ce système, des messages d'autorisations sont envoyés aux décodeurs des utilisateurs. Ces messages contiennent, de façon conventionnelle, les droits d'accès aux événements de télévision à péage. Ils contiennent en outre des pointeurs
25 qui indiquent un emplacement permettant d'obtenir des informations additionnelles. Ces informations additionnelles peuvent être en particulier des informations en clair concernant les événements eux-mêmes ou des logiciels. Ces informations sont liées au décodeur et sont généralement accessibles sans déchiffrement. Elles ne sont pas contenues dans les
30 messages d'autorisation. Ce système ne permet pas de gérer les aspects

de sécurité liés aux données complémentaires et ne permet pas de gérer des conditions d'accès variables en fonction des droits existants pour chaque utilisateur, ces conditions d'accès devant par principe être sécurisées.

- 5 La présente invention se propose de pallier les inconvénients des dispositifs de l'art antérieur en réalisant un dispositif dans lequel il est possible de gérer des droits complexes en offrant donc une grande souplesse d'utilisation à un diffuseur.

Ce but est atteint par un procédé de gestion de l'affichage de descriptifs d'événements à accès conditionnel, comportant les étapes suivantes:

- 10
- envoi de données formant un guide électronique de programmes (EPG), à un décodeur (STB), ce guide électronique étant destiné à l'affichage des événements qui seront diffusés, ces données comportent, pour chaque événement, au moins un identifiant, des données textuelles et un bloc conditionnel comprenant les conditions requises pour l'accès à cet événement,
 - 15 - envoi d'au moins un message d'autorisation (EMM) à un module de sécurité (SC) associé au décodeur, ce message définissant des droits d'accès à un événement;
- 20 caractérisé en ce que le procédé comporte en outre les étapes suivantes:
- envoi audit module de sécurité (SC), du bloc conditionnel (PECM),
 - traitement, dans le module de sécurité, de la condition d'accès contenue dans ledit bloc conditionnel (PECM), et
 - 25 - renvoi par le module de sécurité d'un message indiquant, en fonction de la condition d'accès pour chaque événement et des droits d'accès contenus dans le module de sécurité, si le droit est présent ou non pour chaque événement dans le module de sécurité.

La présente invention et ses avantages seront mieux compris en référence à la description d'un mode de réalisation particulier et aux dessins annexés, dans lesquels :

- 5 – la figure 1 illustre schématiquement un mode de réalisation d'un guide électronique EPG selon l'art antérieur;
- la figure 2 illustre schématiquement le contenu d'un message de contrôle ECM utilisé dans le mode de réalisation de la figure 1;
- la figure 3 illustre le contenu d'un message de contrôle ECM selon la présente invention;
- 10 – la figure 4 illustre le contenu d'un bloc conditionnel utilisé dans le système selon l'invention; et
- la figure 5 représente un mode de réalisation d'un guide électronique EPG selon l'invention.

15 Les figures 1 et 2 décrivent des systèmes connus de l'art antérieur. Dans ces systèmes, les données composant le guide électronique de programme EPG sont transmises par un canal de service et se composent d'informations horaires et textuelles, telles que notamment le titre de l'événement, un descriptif et éventuellement des commentaires. Les données de l'EPG contiennent également le service auquel cet événement
20 est rattaché en terme de droit d'accès, les services étant référencés par exemple de S1 à S48.

Parallèlement, l'événement diffusé est accompagné par les messages de contrôle ECM qui contiennent un certain nombre de champs prédéfinis, portant les références 11 à 14 sur la figure 2, tels que notamment
25 l'identifiant de l'événement (champ 13), le service auquel il est rattaché (champ 14), le mot de contrôle CW (champ 11), l'heure et la date de diffusion (champ 12) et éventuellement, un crédit associé à l'événement. Grâce à cette structure prédéfinie par des champs, la structure du

message est définie de telle sorte que par exemple dans le champ 14, l'on va toujours trouver le numéro d'un service SID.

Ce service est initialisé par un message d'autorisation EMM qui a pour but de définir un bloc d'abonnement dans le module de sécurité SC, ce bloc contenant entre autre la durée de validité de ce service.

Pour afficher le guide électronique EPG sur le téléviseur d'un utilisateur, le décodeur STB lit les droits contenus dans le module de sécurité SC c'est-à-dire les blocs définis plus haut. Plus précisément, il détermine, d'après ces droits, la liste des services disponibles ainsi que la durée ou la date de validité de chaque service. Le décodeur dispose donc d'une part d'une base de données provenant du module de sécurité et contenant la liste des services disponibles avec leur durée de validité et d'autre part, d'une base de données destinées à l'EPG, qui contient la liste des événements, le service auquel il est rattaché et la date de diffusion.

Pour chaque événement, le décodeur peut donc vérifier si le module de sécurité dispose du droit pour le service considéré et si ce droit sera valide au moment de la diffusion de l'événement. En fonction de la réponse de cette comparaison, l'événement sera affiché dans l'EPG, par exemple en rouge si le droit n'est pas acquis et en vert si ce droit est acquis et donc présent dans le module de sécurité.

Sur la figure 1, un "Yes" est affiché dans la dernière colonne de l'EPG en regard de l'événement considéré si le droit pour cet événement est acquis et un "No" dans le cas contraire.

Au moment de la diffusion d'un événement, les messages de contrôle ECM, contenant des mots de contrôle CW et associés à cet événement, sont traités dans le module de sécurité de façon à vérifier l'existence de droits associés à cet événement. Si les droits sont présents, chaque message de contrôle ECM est traité de façon à en extraire les mots de contrôle CW qu'il contient. Ce mot de contrôle est alors envoyé au

décodeur qui déchiffre alors les données qui ont été chiffrées avec ce mot de contrôle spécifique.

Ce mode de réalisation fonctionne parfaitement lorsque les conditions sont simples, par exemple lorsqu'un utilisateur est abonné à un bouquet de services. Dans ce cas, le décodeur compare le contenu de champs prédéfinis dans les informations composants l'EPG avec le contenu de la mémoire du module de sécurité et obtient une réponse directement exploitable.

Lorsque l'on souhaite proposer des offres promotionnelles notamment, il peut être nécessaire de définir des conditions complexes, pour lesquelles une structure fixe prédéfinie de champs ne se révèle pas adaptée. Un exemple d'une telle offre promotionnelle consiste à permettre un accès libre à un bouquet de canaux, le jour anniversaire de chaque abonné. Avec un système conventionnel, une telle offre peut être proposée, mais au prix d'une grande complexité. En effet, pour permettre ceci, il est nécessaire de créer des droits supplémentaires, plus précisément 365 blocs d'abonnement, correspondant chacun à un jour de l'année. Ces droits sont gérés comme les autres droits, ce qui signifie qu'ils sont transmis par des messages d'autorisation EMM. Ces messages doivent être envoyés de façon répétitive à tous les bénéficiaires, de façon à s'assurer que ceux-ci ont bien reçu les droits.

A la réception de ce message, un nouveau bloc d'abonnement sera créé dans le module de sécurité pour cette seule utilisation. Il est à noter que ces messages vont accaparer de la bande passante et des moyens cryptographiques en particulier du fait que le niveau de chiffrement de ces messages est élevé.

Un autre exemple d'offre promotionnelle consiste à facturer un événement donné selon plusieurs montants différents en fonction du type d'abonnement souscrit. Le titulaire d'un abonnement portant sur des chaînes thématiques sportives peut par exemple payer un match de

football à un prix déterminé, alors que les personnes n'ayant pas ce type d'abonnement doivent payer un autre montant pour ce même match. Dans l'état actuel, il n'est pas possible de gérer ce type de règles parce que l'identification de l'événement est rigoureusement identique pour tous les utilisateurs, alors que les conditions d'accès à cet événement dépendent de l'événement et des paramètres propres à un utilisateur.

Aujourd'hui, selon l'état de la technique, la solution consisterait à envoyer un message d'autorisation EMM propre à chaque utilisateur avec le montant de l'événement compte tenu de ses conditions propres. On imagine aisément le nombre de messages à transmettre pour satisfaire tous les utilisateurs.

De façon plus générale, pour pouvoir appliquer des conditions particulières pour un événement particulier, il est nécessaire d'avoir prévu ces conditions par avance dans l'abonnement des utilisateurs concernés. Si tel n'est pas le cas, la gestion des cas particuliers peut se révéler difficile voire impossible. Dans tous les cas, pour générer des droits particuliers sur le module de sécurité, il est nécessaire d'envoyer des messages d'autorisation EMM, à une fréquence suffisante pour s'assurer que la majorité des utilisateurs a bien reçu les droits qui lui sont destinés.

Ce mode de réalisation est peu commode du fait qu'il encombre la mémoire de façon importante et que le trafic des messages d'autorisation EMM utilise inutilement la bande passante disponible.

Dans la figure 3 qui décrit un mode de réalisation de l'invention, le message de contrôle ECM contient non plus une donnée à un emplacement prédéfini, mais une opération Op. Celle-ci est écrite sous forme d'une requête, en utilisant par exemple un langage syntaxique tel que celui connu sous l'acronyme SQL (Structured Query Language).

Le présente invention est particulièrement avantageuse par rapport aux systèmes connus de l'art antérieur par le fait que les conditions définies par des requêtes du type SQL peuvent être imaginées, modifiées ou utilisées

de façon très souple, à n'importe quel moment. Le fait de s'affranchir de champs de données prédéfinis dans les messages de contrôle ECM ouvre la voie à des combinaisons auxquelles l'on n'avait pas pensé lors de la mise en route du système et qui n'étaient par conséquent pas prévues dans l'abonnement des utilisateurs.

Cette gestion simplifiée a comme conséquence de permettre de proposer des offres très diversifiées, même pour un groupe de personnes très restreint. Il est donc possible de générer des offres très ciblées collant au plus près les visions marketing de l'entreprise.

Lors du traitement d'un tel message de contrôle ECM, l'opération Op est traitée par le moteur SQL du module de sécurité SC et du résultat dépendra le renvoi ou non du mot de contrôle CW contenu dans ce même message.

De même que pour les messages de contrôle ECM, il est également prévu, dans le cadre de l'invention, de remplacer les champs d'un message d'autorisation EMM par une requête de type SQL.

Les données mémorisées dans le module de sécurité, définissant les blocs d'abonnement, restent inchangées, seules les opérations sur ces données changent.

A titre d'exemple, une requête de ce type pourrait être :

- Service S22 valide ou Date anniversaire = 10 octobre.

Un autre exemple de requête complexe pour un achat impulsif pourrait être :

- Si le module de sécurité contient les droits pour les services S1, S8 et S12, déduire un montant de 4 USD pour l'événement Ev 1, sinon, déduire un montant de 5 USD pour cet événement.

Dans ce mode de réalisation, le décodeur STB n'est pas habilité à traiter une requête complexe en langage SQL, ceci pour des raisons de sécurité prioritairement.

Dans le cadre de cette invention, la solution consiste à modifier des données transmises à l'EPG, cette modification consistant à inclure dans ces données un nouveau bloc qui est une copie partielle du message de contrôle ECM qui sera transmis avec l'événement considéré.

Ce bloc dénommé bloc conditionnel (PECM) va comprendre au moins la même requête SQL que le message de contrôle duquel il est dérivé. Selon l'implémentation choisie, les autres champs tels que le mot de contrôle pourront être supprimés. Il est clair que les messages de contrôle ECM sont transmis au moment où l'événement est visualisé par l'utilisateur, puisqu'ils contiennent les mots de contrôle CW. Par contre, les blocs conditionnels doivent être envoyés à l'avance puisqu'ils sont utilisés pour former l'EPG qui permet à l'utilisateur de visualiser à l'avance, les droits qu'il a déjà acquis et ceux qu'il peut acquérir.

Lors de la réception de ces données par l'EPG, ce bloc PECM sera transmis au module de sécurité, qui lui, est capable de traiter des requêtes complexes, notamment en langage SQL.

Ce bloc PECM est illustré par la figure 4. Le module de sécurité traitera ce bloc conditionnel de façon conventionnelle et pourra en extraire la requête SQL. Les conditions définies dans cette requête sont analysées dans le module de sécurité et le résultat de la requête est retransmis au décodeur STB. Grâce à ce résultat, l'EPG peut être affiché de la façon expliquée précédemment, en référence à la description de l'art antérieur.

Ce processus est représenté schématiquement par la figure 5. De façon plus détaillée, les données permettant de former l'EPG sont transmises au décodeur STB. Un bloc conditionnel PECM, contenant, sous forme de requête SQL, l'opération qui permet de définir les conditions d'accès, est formé puis transmis au module de sécurité SC. Ce module traite la requête

SQL. Les conditions de la requête SQL sont comparées aux droits inscrits dans le module de sécurité, ce qui permet de déterminer pour quels événements, les droits sont acquis ou peuvent être acquis. Ces droits disponibles sont associés aux données de l'EPG. La liste des événements
5 est ensuite affichée sur le téléviseur de l'utilisateur, en distinguant, pour chaque événement si le module de sécurité dispose des droits ou non.

Revendications

1. Procédé de gestion de l'affichage de descriptifs d'événements à accès conditionnel, comportant les étapes suivantes:

- envoi de données formant un guide électronique de programmes (EPG), à un décodeur (STB), ce guide électronique étant destiné à l'affichage des événements qui seront diffusés, ces données comportent, pour chaque événement, au moins un identifiant, des données textuelles et un bloc conditionnel comprenant les conditions requises pour l'accès à cet événement,
- envoi d'au moins un message d'autorisation (EMM) à un module de sécurité (SC) associé au décodeur, ce message définissant des droits d'accès à un événement;

caractérisé en ce que le procédé comporte en outre les étapes suivantes:

- envoi audit module de sécurité (SC), du bloc conditionnel (PECM),
- traitement, dans le module de sécurité, de la condition d'accès contenue dans ledit bloc conditionnel (PECM), et
- renvoi par le module de sécurité d'un message indiquant, en fonction de la condition d'accès pour chaque événement et des droits d'accès contenus dans le module de sécurité, si le droit est présent ou non pour chaque événement dans le module de sécurité,

et en ce que la condition d'accès contenue dans le bloc conditionnel (PECM) est exprimée sous la forme d'une opération (Op) décrite par une requête en un langage structuré.

2. Procédé de gestion selon la revendication 1, caractérisé en ce que la requête est écrite en langage SQL (Structured Query Language).

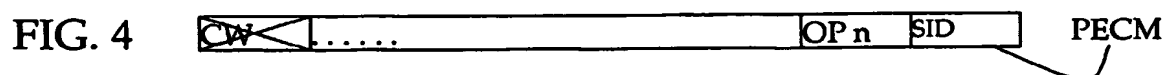
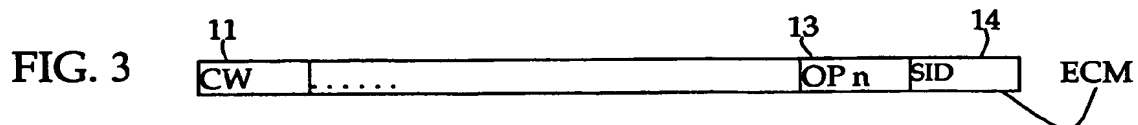
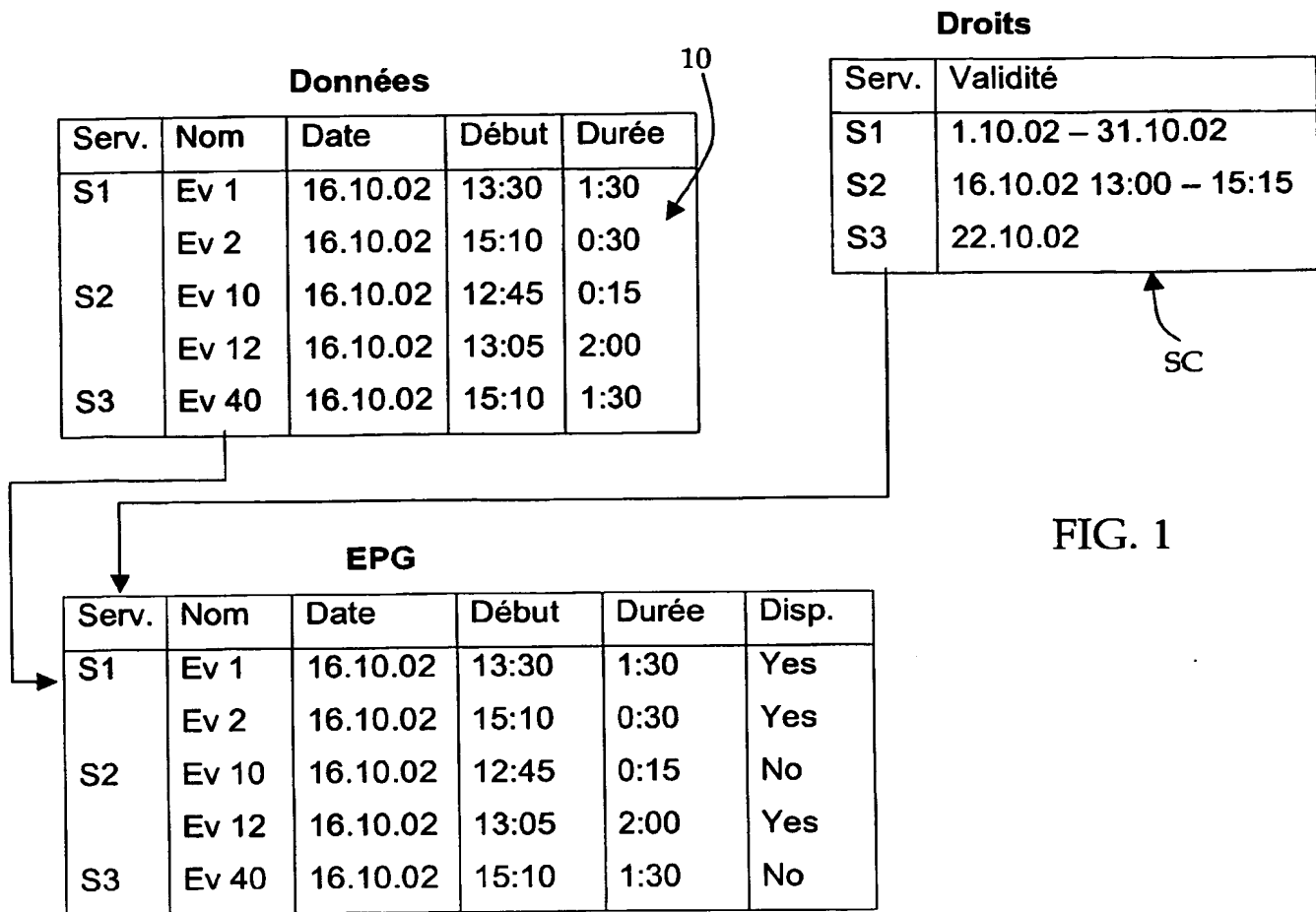
3. Procédé de gestion selon la revendication 1, caractérisé en ce qu'un événement est chiffré par au moins un mot de contrôle (CW), ces mots de contrôle (CW) sont transmis au décodeur (STB) sous la forme d'un

message de contrôle (ECM) chiffré comprenant également les conditions d'accès, ce procédé consistant à transmettre dans le bloc de conditionnel (PECM) tout ou partie du message de contrôle (ECM).

4. Procédé de gestion selon la revendication 3, caractérisé en ce que le bloc conditionnel (PECM) comprend uniquement les données relatives aux conditions d'accès contenues dans le message de contrôle (ECM).

5. Procédé de gestion selon la revendication 4, caractérisé en ce que lesdites données relatives aux conditions d'accès sont envoyées sous forme chiffrée dans le bloc conditionnel (PECM).

6. Procédé de gestion selon la revendication 4, caractérisé en ce que lesdites données relatives aux conditions d'accès sont en clair dans le bloc conditionnel (PECM).



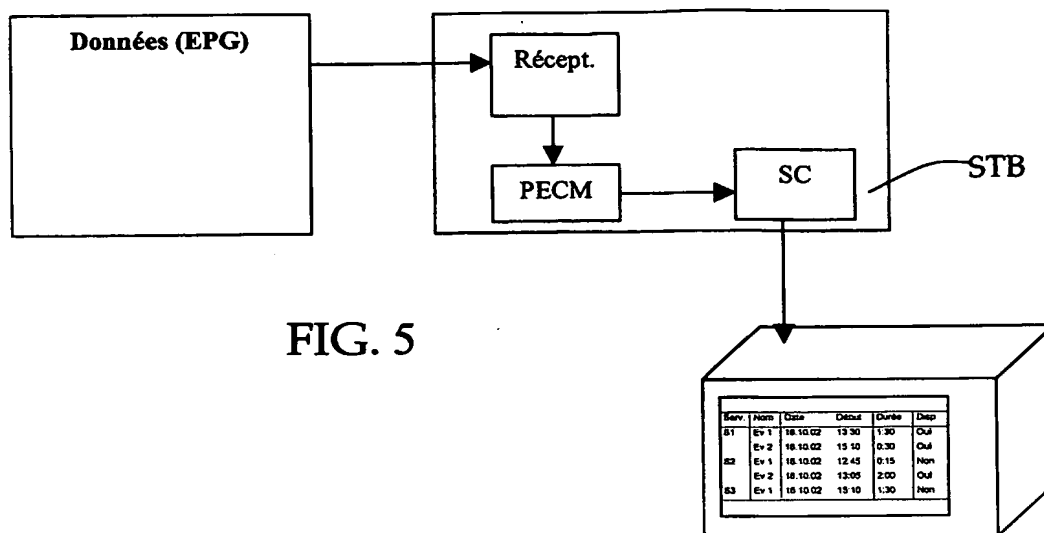


FIG. 5

INTERNATIONAL SEARCH REPORT

International Application No
PCT/IB 03/05654

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04N7/16 H04N7/167

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 97 42762 A (PHILIPS ELECTRONICS NV ;PHILIPS NORDEN AB (SE)) 13 November 1997 (1997-11-13) cited in the application page 3, line 22 -page 4, line 8 page 5, line 14 -page 6, line 24 figures 1,5	1-6
A	WO 02 15578 A (DALLARD NIGEL STEPHEN ;NDS LTD (GB); SMITH NIGEL (GB); CHECHIK DAV) 21 February 2002 (2002-02-21) page 6, line 26 -page 7, line 14	1,3-6
A	GB 2 349 290 A (NDS LTD) 25 October 2000 (2000-10-25) page 12, line 16 -page 14, line 4 page 19, line 3 - line 15 figures 1-3	1,3-6
-/--		

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents:

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

- *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- *G* document member of the same patent family

Date of the actual completion of the international search

17 February 2004

Date of mailing of the international search report

23/02/2004

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2260 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Van der Zaal, R

INTERNATIONAL SEARCH REPORT

International Application No
PCT/IB 02/05654

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	<p>US 5 630 119 A (ARISTIDIS, PHIVOS C. ET AL) 13 May 1997 (1997-05-13) column 4, line 19 - line 63</p> <p>-----</p>	1,2

INTERNATIONAL SEARCH REPORT
Information on patent family members

International Application No
PCT/IB 03/05654

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
WO 9742762	A	13-11-1997	CN 1190516 A	12-08-1998
			EP 0856226 A2	05-08-1998
			WO 9742762 A2	13-11-1997
			JP 11510021 T	31-08-1999
			US 2001005901 A1	28-06-2001
WO 0215578	A	21-02-2002	AU 8244601 A	25-02-2002
			EP 1308043 A1	07-05-2003
			WO 0215578 A1	21-02-2002
			US 2003188154 A1	02-10-2003
GB 2349290	A	25-10-2000	NONE	
US 5630119	A	13-05-1997	NONE	

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°

PCT/IB/88/05654

A. CLASSEMENT DE L'OBJET DE LA DEMANDE IPC 7 H04N7/16 H04N7/167 Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB				
B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE Documentation minimale consultée (système de classification suivi des symboles de classement) IPC 7 H04N Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés) EPO-Internal				
C. DOCUMENTS CONSIDERES COMME PERTINENTS				
Catégorie*	Documents cités avec, le cas échéant, l'indication des passages pertinents	n° des revendications visées		
A	WO 97 42762 A (PHILIPS ELECTRONICS NV; PHILIPS NORDEN AB (SE)) 13 Novembre 1997 (13-11-1997) cité dans l'application page 3, ligne 22- page 4, ligne 8 -page 8, ligne 14 -page 6, ligne 24 -figures 1,5 ---	1-6		
A	WO 02 15578 A (DALLARD NIGEL STEPHEN ; NDS LTD (GB); SMITH NIGEL (GB); CHECHIK DAV) 21 Février 2002 (21-02-2002) page 6, ligne 26 -page 7, ligne 14 ---	1,3-6		
A	GB 2 349 290 A (NDS LTD) 25 Octobre 2000 (25-10-2000) page 12, ligne 16 -page 14, ligne 4 -page 19, ligne 3 -ligne 15 -figures 1-3 ---	1,3-6		
-/--				
<input type="checkbox"/> Voir la suite du cadre C pour la fin de la liste des documents. <input type="checkbox"/> Les documents de familles de brevets sont indiqués en annexe.				
<table style="width: 100%; border: none;"> <tr> <td style="width: 50%; vertical-align: top; border: none;"> * Catégories spéciales de documents cités : "A" document définissant l'état général de la technique, n'étant pas considéré comme particulièrement pertinent "E" document antérieur, mais publié à la date de dépôt international ou après cette date "L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée) "O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens "P" document publié avant la date de dépôt international, mais après la date de priorité revendiquée </td> <td style="width: 50%; vertical-align: top; border: none;"> "T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour permettre de comprendre le principe ou la théorie constituant la base de l'invention "X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément "Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier "&" document qui fait partie de la même famille de brevets </td> </tr> </table>			* Catégories spéciales de documents cités : "A" document définissant l'état général de la technique, n'étant pas considéré comme particulièrement pertinent "E" document antérieur, mais publié à la date de dépôt international ou après cette date "L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée) "O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens "P" document publié avant la date de dépôt international, mais après la date de priorité revendiquée	"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour permettre de comprendre le principe ou la théorie constituant la base de l'invention "X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément "Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier "&" document qui fait partie de la même famille de brevets
* Catégories spéciales de documents cités : "A" document définissant l'état général de la technique, n'étant pas considéré comme particulièrement pertinent "E" document antérieur, mais publié à la date de dépôt international ou après cette date "L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée) "O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens "P" document publié avant la date de dépôt international, mais après la date de priorité revendiquée	"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour permettre de comprendre le principe ou la théorie constituant la base de l'invention "X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément "Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier "&" document qui fait partie de la même famille de brevets			
Date à laquelle la recherche a été effectivement achevée	Date d'expédition du rapport de recherche			
Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé			
n° de télécopieur	n° de téléphone			

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°

PCT/IB 93/05654

C (suite). DOCUMENTS CONSIDERES COMME PERTINENTS		
Catégorie*	Documents cités avec, le cas échéant, l'indication des passages pertinents	n° des revendications visées
A	<p>US 5 630 119 A (ARISTIDIS, PHIVOS C. ET AL) 13 Mai 1997 (13-05-1997) colone 4, ligne 19- ligne 63</p>	1,2

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande Internationale No

PCT/IB 03/03654

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 9742762	A	13-11-1997	CN 1190516 A 12-08-1998
			EP 0856226 A2 05-08-1998
			WO 9742762 A2 13-11-1997
			JP 11510021 T 31-08-1999
			US 2001005901 A1 28-06-2001
WO 0215578	A	21-02-2002	AU 8244601 A 25-02-2002
			EP 1308043 A1 07-05-2003
			WO 0215578 A1 21-02-2002
			US 2003188154 A1 02-10-2003
GB 2349290	A	25-10-2000	AUCUN
US 5630119	A	13-05-1997	AUCUN